



# UNITED STATES PATENT AND TRADEMARK OFFICE

12

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/731,917

12/08/2000

Xin Wang

107146

9895

7590

10/17/2006

Oliff & Berridge PLC  
P.O. Box 19928  
Alexandria, VA 22320

EXAMINER

NGUYEN, THANH T

ART UNIT

PAPER NUMBER

2144

DATE MAILED: 10/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/731,917

Applicant(s)

WANG, XIN

Examiner

Tammy T. Nguyen

Art Unit

2144

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE (3) MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
  - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
  - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
  - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 05 July 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 08 December 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |                                                                                         |                                                                             |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____                                                |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____                                                             | 6) <input type="checkbox"/> Other: _____                                    |



**UNITED STATES PATENT AND TRADEMARK OFFICE**

COMMISSIONER FOR PATENTS  
UNITED STATES PATENT AND TRADEMARK OFFICE  
WASHINGTON, D.C. 20231  
[www.uspto.gov](http://www.uspto.gov)

***Detailed Office Action***

1. This action is in response to the amendment filed on July 5, 2006
2. Claims 1- 13 are pending.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.
4. Claims 1-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro et al., (hereinafter Gennaro) U.S. Patent No. 5,937,066 in view of Markus Jakobsson ., (hereinafter Jakobsson) U.S. Patent No. 6,687,822.
5. As to claim 1, Gennaro discloses the invention substantially as claimed. Gennaro teaches a method for using a document, comprising: issuing a document usage request for using the document in a session [col.13, lines 47-50], (message transmits

- is encrypted and decrypted); authenticating the encrypted document (col.10, lines 51-55); receiving authorization to use the encrypted document (col.10, lines 51-55, and col.25, lines 50-60); receiving session key for the session (col.10, lines 58-62); receiving a proxy key that delegates decryption to the session (col.10, lines 57-67, key encrypting key allowing them to decrypt the encrypted data keys (session key); wherein the session key may be used to decrypt the encrypted document as part of the session rendering process only, thereby assuring that only rendered images of the decrypted document are available to an end user. However, Gennaro does not explicitly disclose partially encrypted and proxy key.
6. In the same field of endeavor, Jakobsson discloses (e.g., a method and system for providing translation certificates). Jakobsson discloses partially encrypted and proxy key (Jakobsson teaches the proxy has the key that allow to decrypt the transcript, each server performs on partial decryption and one partially encryption). [see Jakobsson, col.6, lines 19-27 and col.10, lines 1-16].
7. Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Jakobsson's teaching of a method and system for providing translation certificates with the teachings of Gennaro to have a partially encrypted and proxy key because it would have provided specific techniques to provide for the secure and controlled electronic distribution of documents across a communications network, such as internet.

8. As to claim 2, Gennaro teaches the invention as claimed, further comprising:  
retrieving terms and conditions of the session; retrieving usage parameters and system resource information for the session; and comparing the retrieved usage parameters and system resources and the retrieved terms and conditions, wherein the authorized usage is based on comparison results of the retrieved usage parameters and system resources and the retrieved terms and conditions (col.10, lines 51-67).
9. As to claim 3, Gennaro teaches the invention as claimed, wherein the retrieved terms and conditions are associated with at least one of identification of the encrypted document and usage type (col.14, lines 35-38). However, Gennaro does not explicitly disclose partially encrypted.
10. In the same field of endeavor, Jakobsson discloses (e.g., a method and system for providing translation certificates). Jakobsson discloses partially encrypted (Jakobsson teaches each server performs on partial decryption and one partially encryption). [see Jakobsson, col.6, lines 19-27 and col.10, lines 1-16].
11. Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Jakobsson's teaching of a method and system for providing translation certificates with the teachings of Gennaro to have a partially encrypted because it would have provided specific techniques to provide for the secure and controlled electronic distribution of documents across a communications network, such as internet.

12. As to claim 4, Gennaro teaches the invention as claimed, wherein the document usage request contains at least one of document identification, usage type, and user identification (col.30, lines 41-55).
13. As to claim 5, Gennaro teaches the invention as claimed, wherein authenticating the protected document comprises at least one of: checking a digital signature associated with the encrypted document; and verifying integrity of each component of the protected document (col.1 1, lines 30-35). However, Gennaro does not explicitly disclose partially encrypted.
14. In the same field of endeavor, Jakobsson discloses (e.g., a method and system for providing translation certificates). Jakobsson discloses partially encrypted (Jakobsson teaches each server performs on partial decryption and one partially encryption). [see Jakobsson, col.6, lines 19-27 and col.10, lines 1-16].
15. Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Jakobsson's teaching of a method and system for providing translation certificates with the teachings of Gennaro to have a partially encrypted because it would have provided specific techniques to provide for the secure and controlled electronic distribution of documents across a communications network, such as internet.

16. As to claim 6, Gennaro discloses the invention substantially as claimed. Gennaro teaches a usage authorization system for using an encrypted document, comprising: a request receiving device that receives a document usage request for using the encrypted document in a session (col.13, lines 47-50, message transmits is encrypted and decrypted); a document processing device that authenticates the encrypted document (col. 10, lines 51-55); a document source that authorizes usage of the encrypted document, and issues a proxy key that delegates decryption to the session (col.10, lines 57-67, key encrypting key allowing them to decrypt the encrypted data keys (session key)); an access device that, along with the document device, creates a session key for the session, wherein the session key may be used to decrypt the partially encrypted document as part of the session rendering process only, thereby assuring that only rendered images of the decrypted document are available to an end user. However, Gennaro does not explicitly disclose partially encrypted and proxy key.
17. In the same field of endeavor, Jakobsson discloses (e.g., a method and system for providing translation certificates). Jakobsson discloses partially encrypted and proxy key (Jakobsson teaches the proxy has the key that allow to decrypt the transcript, each server performs on partial decryption and one partial encryption). [see Jakobsson, col.6, lines 19-27 and col.10, lines 1-16].
18. Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Jakobsson's teaching of a method and system for providing translation certificates with the teachings of

Gennaro to have a partially encrypted and proxy key because it would have provided specific techniques to provide for the secure and controlled electronic distribution of documents across a communications network, such as internet.

19. As to claim 7, Gennaro teaches the invention as claimed, wherein the document source retrieves terms and conditions of the session, retrieves usage parameters and system resource information for the session, and compares the retrieved usage parameters and system resources and the retrieved terms and conditions, the authorized usage being based on comparison results of the retrieved usage parameters and system resources and the retrieved terms and conditions (col.10, lines 51-67).
20. As to claim 8, Gennaro teaches the invention as claimed, wherein the retrieved terms and conditions are associated with at least one of identification of the encrypted document and usage type (col. 14, lines 35-38). However, Gennaro does not explicitly disclose partially encrypted.
21. In the same field of endeavor, Jakobsson discloses (e.g., a method and system for providing translation certificates). Jakobsson discloses partially encrypted (Jakobsson teaches each server performs on partial decryption and one partially encryption). [see Jakobsson, col.6, lines 19-27 and col.10, lines 1-16].
22. Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Jakobsson's teaching of a method and system for providing translation certificates with the teachings of



- Gennaro to have a partially encrypted because it would have provided specific techniques to provide for the secure and controlled electronic distribution of documents across a communications network, such as internet.
23. As to claim 9, Gennaro teaches the invention as claimed, wherein the document usage request contain at least one of document identification, usage type, and user identification (col.30, lines 41-55).
24. As to claim 10, Gennaro teaches the invention as claimed, wherein the document processing device authenticates the protected document by at least one of: checking a digital signature associated with the encrypted document; and verifying integrity of each component of the encrypted document (col.11, lines 30-35). However, Gennaro does not explicitly disclose partially encrypted.
25. In the same field of endeavor, Jakobsson discloses (e.g., a method and system for providing translation certificates). Jakobsson discloses partially encrypted (Jakobsson teaches each server performs on partial decryption and one partially encryption). [see Jakobsson, col.6, lines 19-27 and col.10, lines 1-16].
26. Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Jakobsson's teaching of a method and system for providing translation certificates with the teachings of Gennaro to have a partially encrypted because it would have provided specific

- techniques to provide for the secure and controlled electronic distribution of documents across a communications network, such as internet.
27. As to claim 11, Gennaro teach the invention as claimed, comprise a combination of performing partial rendering transformation (col.5, lines 45-65).
28. As to claim 12, Gennaro teaches the invention as claimed, wherein the session and proxy keys are not usable for directly decrypting the encrypted document without rendering the encrypted document and performing proxy transformation on the rendered document (16, lines 45-50). However, Gennaro does not explicitly disclose partially encrypted.
29. In the same field of endeavor, Jakobsson discloses (e.g., a method and system for providing translation certificates). Jakobsson discloses partially encrypted (Jakobsson teaches each server performs on partial decryption and one partially encryption). [see Jakobsson, col.6, lines 19-27 and col.10, lines 1-16].
30. Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Jakobsson's teaching of a method and system for providing translation certificates with the teachings of Gennaro to have a partially encrypted because it would have provided specific techniques to provide for the secure and controlled electronic distribution of documents across a communications network, such as internet.

31. As to claim 13, Gennaro discloses the invention substantially as claimed. Gennaro teaches a method for using a partially encrypted document, comprising: receiving a document usage request for using the encrypted document in a session [col.13, lines 47-50]; authorizing use the encrypted document (col.10, lines 51-55); creating a session key for the session, and issuing a proxy key that delegates decryption to the session (col.10, lines 57-67, key encrypting key allowing them to decrypt the encrypted data keys (session key), wherein the session key enable: rendering a non-encrypted portion of the partially encrypted document; performing a proxy transformation on the partially rendered, partially encrypted document(col.10, lines51-55, and col.25, lines 50-60); and decrypting the proxy transformed, partially rendered, partially encrypted document using the session key, wherein the session key may be used to decrypted the a partially encrypted document as part of the session rendering process only, thereby assuring that only rendered images of the decrypted document are available to an end user. However, Gennaro does not explicitly disclose partially encrypted and proxy key.
32. In the same field of endeavor, Jakobsson discloses (e.g., a method and system for providing translation certificates). Jakobsson discloses partially encrypted and proxy key (Jakobsson teaches the proxy has the key that allow to decrypt the transcript, each server performs on partial decryption and one partially encryption). [see Jackobsson, col.6, lines 19-27 and col.10, lines 1-16].
33. Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Jackobsson's teaching of

a method and system for providing translation certificates with the teachings of Gennaro to have a partially encrypted and proxy key because it would have provided specific techniques to provide for the secure and controlled electronic distribution of documents across a communications network, such as internet.

***Response to Arguments***

34. Applicant's arguments filed on July 5, 2006 have been fully considered, however they are not persuasive because of the following reasons:
35. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "how to securely view the document once the document is received") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).
36. Examiner maintain the rejection because Gennaro and Jakobsson disclose proxy key as shown in Jakobsson col.6, lines 20-21 (the proxy has the key that allows him to decrypt the transcript) and session key as shown in Gennaro col.11, lines 29-36 (the encrypted escrowed record containing the self-identification and password is also provided to the escrow agent. The escrow agent decrypted the escrow record with its private part of the key, validates the credentials against the self-identification data , and provides the password to the user only if the user is properly verified), they do the decrypt the partially encrypted document as shown in Jakobsson col.10, lines 5-6

(partial decryption). Gennaro and Jakobsson clearly show the invention claimed application. Examiner sees no where in the pending claims shows preventing a decrypted copy of the transferred document from being available for electronic copying by an intruder, or intended recipient.

37. Therefore, the Examiner asserts that cited prior arts teach or suggest the subject matter broadly recited in independent claims 1, 6, and 13. Claims 2-5, 7-12 are also rejected at least by the virtue of their dependency on independent claims and by other reasons set forth in the previous office action.

38. Accordingly, claims 1-13 are respectfully rejected.

### ***Conclusion***

39. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

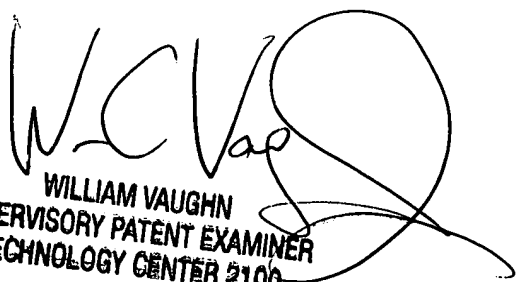
40. Any inquiry concerning this communication or earlier communications from

the examiner should be directed to Tammy T. Nguyen whose telephone number is 571-272-3929. The examiner can normally be reached on Monday - Friday 8:30 - 5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, *William Vaughn* can be reached on 571-272-3922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TNN  
September 29, 2006

  
WILLIAM VAUGHN  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100